**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:** March 10, 2024 | Emotet.exe |
| Description | Analyzing Emotet.exe for Possible Malicious Activities |
| Tool(s) used | Wireshark |
| The 5 W's | * **Who**: A process named Emotet.exe was running as root * **What**: This was discovered to be a Banking Trojan * **Where**: This incident occurred in one of TedprimeHub’s outlet machine * **When**: Between the hours of 2:00Hr and 5:00Hr GMT+1 * **Why**: This attack must have been due to a discovered server misconfiguration. After a successful infiltration, a Command and Control (C2) server with the IP Address of 10.1.6.206 was ex-filtrating company’s sensitive data through a compromised public server with the IP Address of 87.252.164.58, which then further exposed the internal network including IP Addresses 66.153.205.191, 173.255.195.246, 103.92.235.25 and 5.2.136.39 communicating with the C2 server. |
| Additional notes | 1. Proper reconfiguration of server and host be made, and patches be updated. 2. Firewall, IDS/IPS, with Anti-Virus be given priority. 3. Proper network monitoring should be up-scaled. |